



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/676,231

09/30/2003

Stephen R. Carter

1565.060US1

6382

21186

7590

12/03/2009

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.

P.O. BOX 2938

MINNEAPOLIS, MN 55402

EXAMINER

BLAIR, DOUGLAS B

ART UNIT

PAPER NUMBER

2442

NOTIFICATION DATE

DELIVERY MODE

12/03/2009

ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@slwip.com

request@slwip.com



Art Unit: 2442

## **DETAILED ACTION**

### ***Response to Amendment***

The applicant has amended claims 8, 9, and 21. Claims 8-14 and 21-29 are currently pending.

### ***Response to Arguments***

Applicant's arguments filed 7/29/2009 have been fully considered but they are not persuasive. The applicant is directed towards paragraph 140 of Amdur which shows a tripartite relationship between the various users, services (scalability of security service), and the resources. The applicant's specification does not limit the term "contract" in any specific way and does not provide and specifics as to the implementation of the tripartite relationship so the amendments do not overcome what is already taught in Amdur.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 8-14 and 21-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication Number 2008/0134286 by Amdur et al. in view of U.S. Patent Number 6,072,875 to Tsudik.

As to claim 8, Amdur teaches a method implemented in a computer-readable medium and for executing on a proxy server (Fig. 3 embodiment) the method for policy and attribute based access to a resource, comprising: receiving, at the proxy server, a session request for access to a resource, wherein the session request is sent from a service and includes alias identity information for a principal (paragraph 94, the user's login name is considered the alias or alternatively the biometric data in paragraph 188 can be considered an alias), wherein the alias identity information includes a password and a principal identification (paragraph 188 mentions a password and identification); mapping, by the proxy server, the alias identity information to identity information of the principal, the identity information associated with the true identity of the principal whereas the alias identity information is the password and the principal identification and the identity information and the true identity of the principal available to the proxy server by not the service or the resource (paragraphs 95-96); authenticating, by the proxy server, the identity information; acquiring, by the proxy server, a service contract for the principal, the service, and the resource, obtaining the service contract selective resource access policies and attributes which are permissibly used by the service when accessing the resource on behalf of the principal (paragraphs 95-96); defining, via the service contract, a tripartite relationship among the principal, the service, and the resource, the service contract is derived from an identity configuration of the principal (paragraph 140); and establishing, by the proxy server, a session with the service, wherein the session is controlled by the service contract (paragraphs 95-96); however Amdur does not explicitly teach alias information that is randomly generated from identity information that identifies the true identity of the principal.

Art Unit: 2442

Tsudik teaches a method wherein alias information that is randomly generated from identity information that identifies the true identity of the principal (see abstract and corresponding disclosure. The encrypted identifier and password are considered randomized).

It would have been obvious to one of ordinary skill in the Computer Networking art at the time of the invention to combine the teachings of Amdur regarding using a proxy to authenticate users with the teachings of Tsudik regarding randomized alias identification because such randomization prevents an intruder from detecting a user's identity or moves though the network.

As to claim 9, Amdur teaches the method of claim 8 further comprising accessing an identity configuration for the principal in order to acquire the selective resource access policies and attributes included within the service contract (paragraph 96).

As to claim 10, Amdur teaches the method of claim 8 further comprising denying access attempts made by the service during the session when the access attempts are not included within the service contract (paragraphs 95-96).

As to claim 11, Amdur teaches the method of claim 8 further comprising terminating the session when an event is detected that indicates the service contract is compromised or has expired (paragraphs 198-199).

As to claim 12, Amdur teaches the method of claim 8 further comprising establishing the service contract with the principal prior to receiving the session request (paragraphs 95-96).

As to claim 13, Amdur teaches the method of claim 12 further comprising reusing the service contract to establish one or more additional sessions with the service, wherein the one or more additional sessions are associated with one or more additional session requests made by the service (paragraphs 93-96).

Art Unit: 2442

As to claim 14, Amdur teaches the method of claim 12 wherein the establishing further includes establishing the service contract with the principal in response to a redirection operation performed by a proxy that intercepts a browser request issued from the principal to the service for purposes of accessing the resource (paragraph 88).

Claim 21 is rejected for the same reasoning as claim 8.

As to claim 22, Amdur teaches the policy and attribute based resource session manager of claim 21 having instructions further comprising, permitting the service to indirectly access an identity store which represents the resource, and wherein the identity store includes secure information related to the principal (paragraphs 95-96).

As to claim 23, Amdur teaches the policy and attribute based resource session manager of claim 21 having instructions further comprising terminating the session when the service contract expires or is compromised (paragraphs 198-199).

As to claim 24, Amdur teaches the policy and attribute based resource session manager of claim 21, wherein the requesting of the mapping further includes interacting with an alias translator (paragraphs 95-96).

As to claim 25, Amdur teaches the policy and attribute based resource session manager of claim 21, wherein the requesting of authentication further includes interacting with an identification authenticator (paragraphs 95-96).

As to claim 26, Amdur teaches the policy and attribute based resource session manager of claim 21 having instructions further comprising managing the session by acting as an

Art Unit: 2442

intermediary between the service and a legacy Lightweight Directory Access Protocol (LDAP) application which has access privileges to the resource (paragraphs 97-103).

As to claim 27, Amdur teaches the policy and attribute based resource session manager of claim 26, wherein the receiving further includes intercepting a session request that is issued from the service for the legacy LDAP application, wherein the session request includes the alias identity information (paragraphs 97-103).

As to claim 28, Amdur teaches the policy and attribute based resource session manager of claim 27 having instructions further comprising managing the session with respect to the service as if the policy based resource session manager were the legacy LDAP application (paragraphs 97-103).

As to claim 29, Amdur teaches the policy and attribute based resource session manager of claim 21 wherein the instructions for establishing the session further includes defining the selective resource access policies as at least one of a read operation and a write operation and defining the attributes as selective confidential data related to the principal, wherein the policies define operations that are permissible on the attributes, and wherein values for the attributes reside in the resource (paragraphs 95-96).

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2442

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DOUGLAS B. BLAIR whose telephone number is (571)272-3893. The examiner can normally be reached on 9:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571) 272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Application/Control Number: 10/676,231

Page 8

Art Unit: 2442

/Douglas B Blair/

Primary Examiner, Art Unit 2442